Software Test Report
For
Network Monitoring and Management
Hybrid MANET Dynamic Addressing

Contract Number N00014-04-C-0179
CDRL B005

Submitted to:
Office of Naval Research
875 North Randolph Street
Suite 1425
Arlington, VA 22203-1995

24 July 2007

Submitted by:
Science Applications International Corporation (SAIC)
1710 SAIC Drive
McLean, VA 22102-3703

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 24-07-2007	**2. REPORT TYPE** Software Test Report	**3. DATES COVERED** *(From - To)* 19-07-2006 – 21-11-2007

4. TITLE AND SUBTITLE
Software Test Report
For the Network Monitoring and Management

Hybrid MANET Dynamic Addressing

5a. CONTRACT NUMBER
N00014-04-C-0179

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Dr. David Sutkoff
Jerilyn McElwee

Brad Gaspard

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Science Applications
International Corporation
(SAIC)

1710 SAIC Drive
McLean, VA 22102-3703

8. PERFORMING ORGANIZATION REPORT NUMBER
HMDA-STR-01-U-R0C1

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Office of Naval Research

875 North Randolph Street
Suite 1425
Arlington, VA 22203-1995

10. SPONSOR/MONITOR'S ACRONYM(S)
ONR

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The objective of this applied research project was to create a service that allows mobile nodes in a hybrid MANET to receive global Internet Protocol IP addresses from the appropriate mobile gateway without requiring user configuration. A MANET is a mobile ad-hoc network communicating via wireless links. A hybrid MANET adds one or more gateway nodes (e.g. nodes providing connectivity to other networks via satellite or other links).

A Hybrid MANET Dynamic Addressing (HMDA) service was developed which provides a method for gateway discovery and dynamic global IP address configuration of mobile nodes. This service will allow mobile nodes to roam seamlessly from one area to another providing continuous communications throughout all network merges and partitions.

SAIC has successfully implemented and demonstrated the Network Monitoring and Management Hybrid MANET Dynamic Addressing service that meets or exceeds the requirements and objectives set forth by ONR. The HMDA service was demonstrated using two gateways and six mobile nodes distributed across two subnets. Since positive test results were obtained, it is recommended to transition this methodology from the lab environment to an operational scenario.

15. SUBJECT TERMS
Dynamic Addressing, MANET, Hybrid MANET, Autoconfiguration, HMDA, ONR

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Jerilyn McElwee
a. REPORT UU	**b. ABSTRACT** UU	**c. THIS PAGE** UU	SAR	28	**19b. TELEPHONE NUMBER** *(include area code)* 703 676 2107

Revision Record

Revision R0C0 is the initial release of the Network Monitoring and Management Hybrid Mobile Ad-hoc Network (MANET) Dynamic Addressing (HMDA) Software Test Report (STR). Subsequent releases will have a unique revision number.

Revision	Date	Description
R0C0	July19, 2007	Initial Release.
R0C1	July 24, 2007	Minor Editorial updates

Table of Contents

Section **Page**

1.0 Scope 1
1.1 Identification 1
1.2 System Overview 1
1.3 Document Overview 2
2.0 Referenced Documents 3
2.1 Government Documents 3
2.2 Non-Government Documents 3
3.0 Goals and Implementation Decisions 4
3.1 Goals 4
3.2 Implementation Considerations 5
4.0 Operational Description 7
4.1 OLSR DHCP Relay Solution 7
4.2 HMDA Network Solution 9
4.2.1 Mobile Node HMDA Functions 10
4.2.2 Gateway HMDA Functions 12
5.0 Test Results 13
5.1 Formal Testing 13
5.2 Expanded Testing 20
6.0 Conclusion 22
7.0 Acronyms, Abbreviations, and Definitions 24

List of Figures

Figure **Page**

Figure 1.2-1 Hybrid MANET Dynamic Addressing Test Configuration 1
Figure 4.1-1 OLSR DHCP Relay Network Configuration 8
Figure 4.2-1 HMDA Network Configuration 10
Figure 4.2.1-1 HMDA Mobile Node Components 10
Figure 4.2.2-1 HMDA Gateway Components 12
Figure 5.1-1 Hardware/Software Configuration Test Network Topology 14
Figure 5.1-1a HMDA *myiptables* File 15
Figure 5.1-2 Gateway Mobile Node Initialization Test Network Topology 16
Figure 5.1-3 Gateway Announcement and Discovery Test Network Topology 18
Figure 5.1-4 Mobile Node Reconfiguration and Gateway Selection Test Network Topology 19

List of Tables

Table **Page**

Table 3.0-1 HMDA Design Goals 4
Table 3.2-1 ONR Hybrid MANET Dynamic Addressing Configuration 6

1.0 Scope

1.1 Identification

This Software Test Report (STR) provides a technical analysis, operational description and test results for Hybrid Mobile Ad-Hoc Network (MANET) Dynamic Addressing (HMDA). The Hybrid MANET Dynamic Addressing solution was developed for the Office of Naval Research (ONR) under contract number N00014-04-C-0179.

1.2 System Overview

A MANET is a multi-hop network comprised of mobile nodes communicating via wireless links. A hybrid MANET is a mobile ad-hoc network together with one or more gateway nodes (e.g. nodes providing connectivity to other networks via satellite or other links) which collectively form a multi-hop wireless network.

Hybrid MANET Dynamic Addressing will provide a method of gateway discovery and dynamic global Internet Protocol (IP) address configuration of mobile nodes for a hybrid MANET. This system will allow mobile nodes to roam seamlessly from one area to another providing continuous communications throughout all network merges and partitions.

Hybrid MANET Dynamic Addressing was demonstrated using two gateways and six mobile nodes distributed across two subnets. The environment that was used to verify Hybrid MANET Dynamic Addressing is shown in Figure 1.2-1. The procedures used to verify HMDA functionality can be found in the Hybrid MANET Dynamic Addressing Software Test Plans/Procedures, HMDA-STPP-U-R0C1.

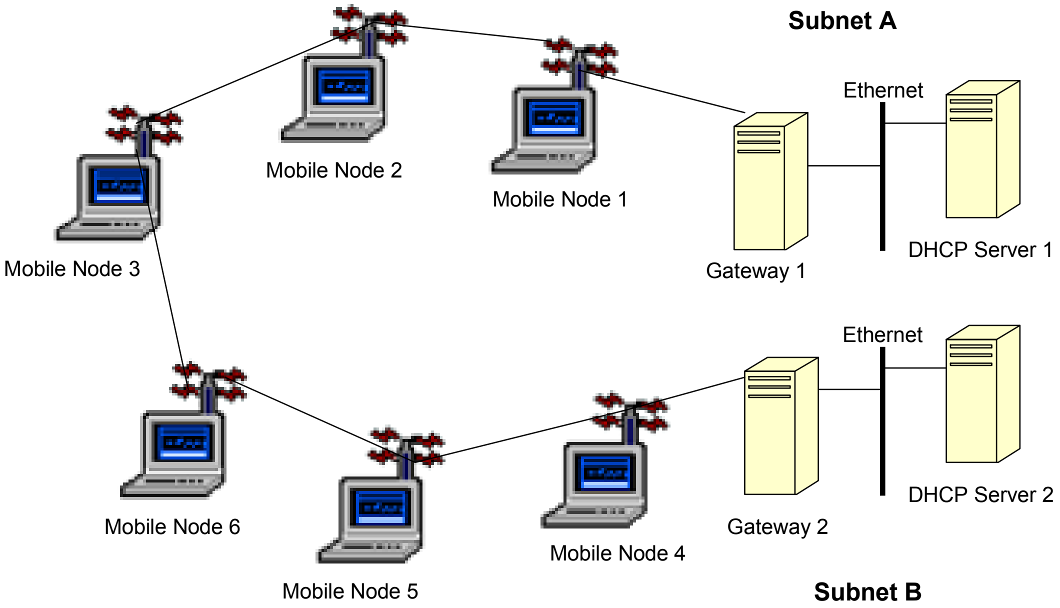

Figure 1.2-1 Hybrid MANET Dynamic Addressing Test Configuration

1.3 Document Overview

This section provides a document overview. Section 2.0 provides a list of references and applicable documents. Section 3.0 discusses the design goals established for the project as well as considerations and trade offs made for project implementation. An operational description and software overview of HMDA is provided in Section 4.0. Section 5.0 describes the formal testing activities and discusses the results of these tests. Section 6.0 summarizes the overall project and identifies additional efforts that should be undertaken to further test and improve the solution for fielding. Section 7.0 includes a list of notes and acronyms applicable to this document.

2.0 Referenced Documents

The following documents of the exact issue shown form a part of this document to the extent specified herein.

2.1 Government Documents

- HMDA Software Test Plans/Procedures, document number HMDA-STPP-01-U-R0C1, dated July 24, 2007.
- HMDA User's Manual, document number HMDA-UM-01-U-R0C1, dated October 19, 2007
- ONR-Final Technical Report, ONR-Final-Report-01-U-R0C0, dated February 7, 2006
- Hybrid MANET Software Requirements Specification document number HMDA-SRS-U-01-R0C0, dated October 19, 2006.

2.2 Non-Government Documents

- RFC 3626 – Optimized Link State Routing Protocol (OLSR)
- RFC 2131 – Dynamic Host Configuration Protocol
- RFC 1533 – DHCP Options and BOOTP Vendor Extensions

3.0 Goals and Implementation Decisions

This section describes the ONR program HMDA design goals and implementation decisions.

3.1 Goals

The goals for implementing Hybrid MANET Dynamic Addressing were established as a result of research and OPNET modeling activities (see ONR-Final Technical Report, ONR-Final-Report-01-U-R0C0, dated February 7, 2006). These design goals are summarized in Table 3.0-1.

Table 3.0-1 HMDA Design Goals

1. Seamlessly determine mobile node/gateway association
2. Provide each mobile node a unique topologically correct address
3. Support topology changes such as partitions and merges
4. Require minimal changes to existing standards-based software
5. Avoid single-points of failure
6. Minimize the amount of configuration and reconfiguration required
7. Support route aggregation in distant networks that connect with the MANET
8. Facilitate local configuration of global IP address and local connections (without requiring expensive satellite bandwidth)
9. Allow nodes to retain their addresses for a configurable interval, even if their associated gateway subsequently becomes unavailable and there are no other gateways in the area. If another gateway is available, nodes should reconfigure.
10. Support address reuse of unused address space
11. Independence of MANET routing protocol
12. Support timely configuration of IP addresses
13. Applicable to Internet Protocol Version 4 (IPv4) and in principle Internet Protocol Version 6 (IPv6)
14. Path lengths should be minimized while maintaining routing stability since Transmission Control Protocol (TCP) performance degrades over multi-hop wireless low-bandwidth links
15. Minimize the influence of auto-configuration overhead traffic on the ongoing MANET communication performance. For example, when some MANET partitions merge, a broadcast storm may occur due to duplicate address detection traffic

The functional requirements defined in the Hybrid MANET Software Requirements Specification (HMDA-SRS-U-01-R0C0) were derived from many of these design goals and formed the basis for design and implementation of Hybrid MANET Dynamic Addressing. The focus of the prototype development was to produce a working dynamic addressing solution in a laboratory environment.

Goals 1, 2, 3, and 13 have been directly implemented. The parameters that allow the optimization to satisfy goals 8, 9, 12, 14, and 15 have been implemented. Some goals (4, 5, and 6) are “good practice” and are always kept in mind when designing operational software. They can be realized as in the case of goal 5 by dual redundancy studies with regards to survivability and single points of failure but as of this time these studies have not been conducted.

Goal 10 is met by the open source Internet Software Consortium (ISC) Dynamic Host Configuration Protocol (DHCP) server (bundled with openSUSE 10.1). It is the responsibility of the DHCP server to reuse unused IP address space.

The goal that was not addressed in HMDA at this time is goal 11, Independence of MANET routing protocols. SAIC selected a routing protocol that is prominently used in the MANET community, Optimized Link State Routing (OLSR). Alternate routing protocols may not work in this solution set. Additional work would be required to adapt the dynamic addressing solution to other protocols. But once a MANET routing protocol like OLSR has been chosen, goal 7 becomes realized.

3.2 Implementation Considerations

The application software required for successful demonstration of Hybrid MANET Dynamic Addressing is shown in Table 3.2-1. ONR HMDA was developed and tested in a laboratory environment. As a result, some of the operational instructions and code is specific to the software components and drivers selected.

An important software selection consideration was how to satisfy the requirement for ‘smart flooding’ of Gateway Announcement messages in a MANET. Two software packages were analyzed: the Simplified Multicast Forwarding (SMF) package developed by the Navy Research Laboratory and an open source implementation of the OLSR protocol called OLSRd[1].

OLSRd was selected for the following reasons:

- Provides a well documented Application Programming Interface (API) that permits the writing of plug-ins (dynamically loaded libraries) which performs specialized functions, like the forwarding of Gateway Announcement messages. There is no need to modify the OLSR daemon. Additionally, plug-ins support Inter-Process Communication (IPC) via a socket interface.
- OLSRd has an active developer and user community along with a mailing list for support on topics ranging from OLSRd configuration to plug-in development.
- OLSRd runs on both Windows (Windows 2000 and XP) and Linux platforms.

The AutoConfigPlug-in needed to be written in a language that could be compiled as a dynamic library. The programming language “C”, which can be compiled, was chosen because the implementation was fairly straightforward and because OLSRd is written in “C”.

The other software component that had to be developed was the AutoConfigServer. This component is responsible for orchestrating several activities including communications with the AutoConfigPlug-in (to obtain the list of available gateways), DHCP messaging to and from the gateway, and the gateway selection process. Python[2] along with the Twisted[3] package is well suited to satisfy these requirements. Python is an object oriented programming language that runs on virtually every hardware platform, comes with extensive standard libraries, and is an extremely productive scripting programming language. Twisted is an asynchronous network

[1] http://www.olsr.org/
[2] http://www.python.org/
[3] http://twistedmatrix.com/trac/

framework for Python. It handles many common protocols and programming tasks like user authentication and includes everything necessary to build the HMDA network application.

The openSUSE distribution of Linux was selected as the development platform (any Linux distribution would have served equally well). The main reason for developing under Linux is its abundance of open source tools like “iptables” (network shaping tool) and Ethereal (a protocol analyzer). These tools simplified development and debugging of the HMDA network application.

The initial concept for this solution required listening and intercepting DCHP Discover broadcast messages and converting them to unicast messages. Because off-the-shelf DHCP clients run as server applications, attempts made to implement this approach required complex invasive methodologies that could not be realized during this contract period. Instead, a HMDA DHCP Client process was developed that allowed the unicasting of DHCP messages as well as ensuring that certain design goals could be met (see section 5.0 for further discussion). The ISC DHCP server is distributed with the openSUSE operating system and as such was used in our laboratory environment. The HMDA DHCP Client is not dependent on this server.

Table 3.2-1 ONR Hybrid MANET Dynamic Addressing Configuration

Configuration Item	Software	Vendor	Description
Gateway	openSUSE v10.1	Open Source	Linux Operating System
	OLSRd v 4.10	Open Source	MANET Routing Protocol
	Python 2.4	Open Source	Object oriented programming language
	Twisted v 2.4	Open Source	Event Driven Networking Framework under Python
	AutoConfig Server	ONR/SAIC	Dynamic Addressing
	AutoConfig Plug-in	ONR/SAIC	Dynamic Addressing
	madwifi v 0.9.2	Open Source	Wireless Card Driver
DHCP Server	openSUSE v10.1	Open Source	Linux Operating System
	ISC DHCP Server v3.03	Open Source	DHCP Server Software
Mobile Node	openSUSE v10.1	Open Source	Linux Operating System
	OLSRd v 4.10	Open Source	MANET Routing Protocol
	Python v 2.4	Open Source	Object oriented programming language
	Twisted v 2.4	Open Source	Event Driven Networking Framework under Python
	AutoConfig Server	ONR/SAIC	Dynamic Addressing
	AutoConfig Plug-in	ONR/SAIC	Dynamic Addressing
	madwifi v 0.9.2	Open Source	Wireless Card Driver

4.0 Operational Description

A phased approach to developing the HMDA network solution was adopted in order to accomplish the mobile node autoconfiguration requirement and then investigate how best to develop the dynamic addressing requirements of gateway selection. The objective was to first build the autoconfiguration portion of the software and than add the dynamic addressing functionality. The first phase proved to hold merit as a standalone process for addressing mobile node autoconfiguration requirements but ultimately was not incorporated into the final solution. This approach is referred to as OLSR DHCP Relay. The OLSR DHCP Relay is a simple auto-configuration methodology. Using the concept of a DHCP Relay as used in wired Local Area Networks (LANs) and applying it to a MANET, OLSR is used to relay DHCP messages between configuring nodes and the DHCP server.

The dynamic addressing solution addresses the requirements of autoconfiguration as well as gateway selection and is referred to simply as HMDA. HMDA is the implementation of the OPNET model developed during the previous contract year. In this implementation configuring nodes, upon bootup, select a temporary random IP address (from a fixed pool of addresses) and then join the OLSR based MANET. It listens for specially formatted OLSR Gateway Announcement messages, sent periodically by the gateways, and selects the gateway that is the fewest hops away. The mobile node then unicasts a DHCP Discover or Request message to this gateway to obtain a globally routable IP address from its DHCP server. It also supports switching to a different gateway to obtain a new IP address if the previously selected gateway is no longer being heard.

A high level overview of the OLSR DHCP Relay solution is provided for information. Both solutions will be delivered.

4.1 OLSR DHCP Relay Solution

The problem that the OLSR DHCP Relay solves is how to efficiently forward DHCP messages between a configuring node and a DHCP server that are effectively separated by one or more subnets. A DHCP Relay agent solves this problem in wired networks where a router or computer straddles two subnets, listens for DHCP messages broadcast on one subnet, and relays those messages to a DHCP server on a different subnet. In a MANET this is not practical. Each mobile node would have to have a DHCP Relay agent running and the result would be a DHCP message storm whose size is dependent upon the number of mobile nodes in the MANET. Using OLSR to forward DHCP messages can reduce the number of DHCP message rebroadcasts by:

- Using OLSR to efficiently ‘smart’ flood the OLSR DHCP messages throughout the MANET.
- Adding a random delay before an OLSR DHCP message is forwarded. A mobile node will only forward the message if another node has not already done so.

The OLSR DHCP Relay AutoConfigServer and AutoConfigPlug-in Software Configuration Items (SCIs) are installed on both the mobile and gateway nodes and perform very similar functions. Figure 4.1-1 depicts these SCIs within the network environment. Both are responsible for relaying DHCP broadcast messages between a configuring node and the DHCP server. The software running on a gateway node has the additional responsibility of relaying requests directly to the DHCP server.

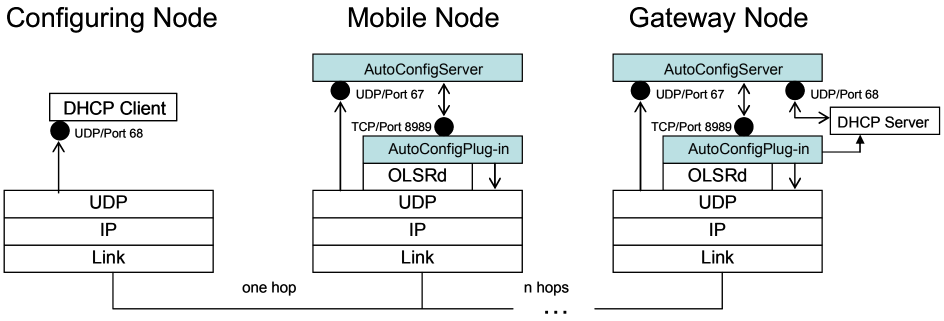

Figure 4.1-1 OLSR DHCP Relay Network Configuration

Just like a node on a wired LAN, a configuring node will broadcast a DHCP Discover or Request[4] message upon bootup. Assuming that the configuring node is within range of at least one other node in the MANET, one or more mobile and/or gateway nodes will hear this request. Mobile nodes and gateway nodes both have servers listening on port 67 (DHCP server port) and will handle the message as follows:

- Mobile node – The AutoConfigServer will wait 0.2 sec – 1.0 sec before establishing a Transmission Control Protocol (TCP) connection to the AutoConfigPlug-in. After this random delay, the AutoConfigServer will forward the DHCP Discover or Request message to the AutoConfigPlug-in.

- Gateway node – The AutoConfigServer will immediately establish a TCP connection to the AutoConfigPlug-in and forward the DHCP Discover or Request message. The DHCP message will also be unicast to the DHCP server after setting the broadcast flag in the DHCP flags field.

The OLSR daemon (with AutoConfigPlug-in) will hear OLSR DHCP messages that have been routed by other nodes over the MANET. Before the AutoConfigPlug-in transmits an OLSR DHCP message throughout the MANET, a check will be made to determine if another mobile node has already forwarded the message and if so, will silently drop it.

If a mobile node decides to transmit the DHCP message as an OLSR DHCP message, it will first strip off the *sname* and *file* fields[5] of the DHCP message, and maintain a record of it so that when the OLSR DHCP response message is heard, the AutoConfigPlug-in will know to broadcast the DHCP response message to the configuring node. As previously stated, the purpose of the random delay is to limit the number of nodes that transmit the same OLSR DHCP message from the configuring node.

[4] If the node is attempting to obtain its previous IP address it will broadcast a DHCP Request message.
[5] Server host name and boot file name respectively. These fields take up a total of 192 bytes and are removed from the OLSR DHCP message for transmission efficiency reasons.

These OLSR DHCP messages will eventually find their way to a gateway node. The gateway AutoConfigPlug-in is responsible for taking the OLSR DHCP message, converting it back to a DHCP message, adding back in the *sname* and *file* fields, setting the broadcast flag in the DHCP flags field, and unicasting it to the DHCP server.

The AutoConfigServer on the gateway node includes a server listening on port 67 for DHCP messages from the DHCP server. It establishes a TCP connection with the AutoConfigPlug-in, sends the DHCP response message from the DHCP server, this DHCP message is converted to OLSR DHCP message as before and OLSR forwards it throughout the MANET. Eventually, it will reach the mobile node that initially forwarded the DHCP request message for the configuring node. The AutoConfig Plug-in for this mobile node then converts the OLSR DHCP message back to a DHCP message and broadcasts the response back to the configuring node.

Once a configuring node obtains an IP address, the OLSRd daemon and AutoConfigServer is started (AutoConfigPlug-in is loaded when the OLSRd daemon is started) and the node joins the MANET and serves as an OLSR DHCP Relay for other configuring nodes. [Note: the functionality to automatically start OLSRd and the AutoConfigServer after receiving an IP address has not been implemented.] Host-based routing is then used to handle IP address lease renewals. If a lease cannot be renewed because the gateway is no longer in range, the DHCP client will eventually broadcast a DHCP Discover message and the process will repeat.

4.2 HMDA Network Solution

HMDA AutoConfigServer and AutoConfigPlug-in SCIs are installed on both the mobile and gateway nodes. However, the functions provided on each type of node are different. Figure 4.2-1 demonstrates how these SCIs interface within the network environment.

The AutoConfigServer software running on a mobile node is responsible for IP address initialization, gateway selection and for providing DHCP client functionality. The mobile node AutoConfigPlug-in software receives and maintains gateway information from all Gateway Announcements messages that are broadcast over the MANET. This information is provided to the AutoConfigServer upon request.

Once a mobile node has been initialized with a temporary IP address, gateway information from the AutoConfigPlug-in is requested and sent to the AutoConfigServer via port 8989. The AutoConfigServer uses this information to send the DHCP Discover and Request messages to the closest gateway.

The AutoConfigServer on the gateway receives the DHCP Discover and Request messages via port 6767 and forwards these messages to the DHCP server via port 68. Response messages from the DHCP server are sent back via the gateway and received by the mobile nodes on port 6767. The gateway AutoConfigPlug-in generates configurable periodic Gateway Announcement messages using the OLSRd routing protocol.

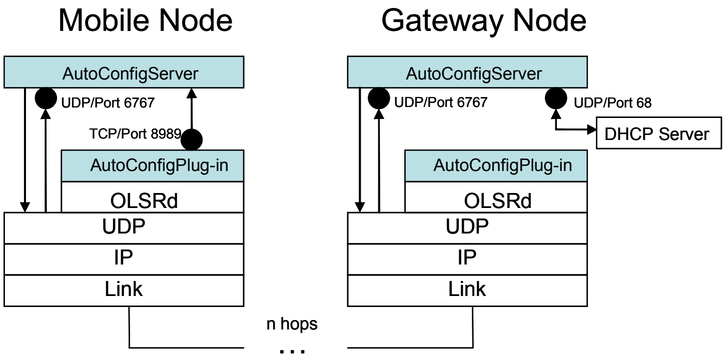

Figure 4.2-1 HMDA Network Configuration

4.2.1 Mobile Node HMDA Functions

The AutoConfigServer and AutoConfigPlug-in software installed on the mobile nodes are essentially a set of processes and services running in parallel. Figure 4.2.1-1 shows the high level functional HMDA components on the mobile node. The AutoConfigServer provides the Initialization, HMDA DHCP Client, and Gateway Selection functionality required for HMDA.

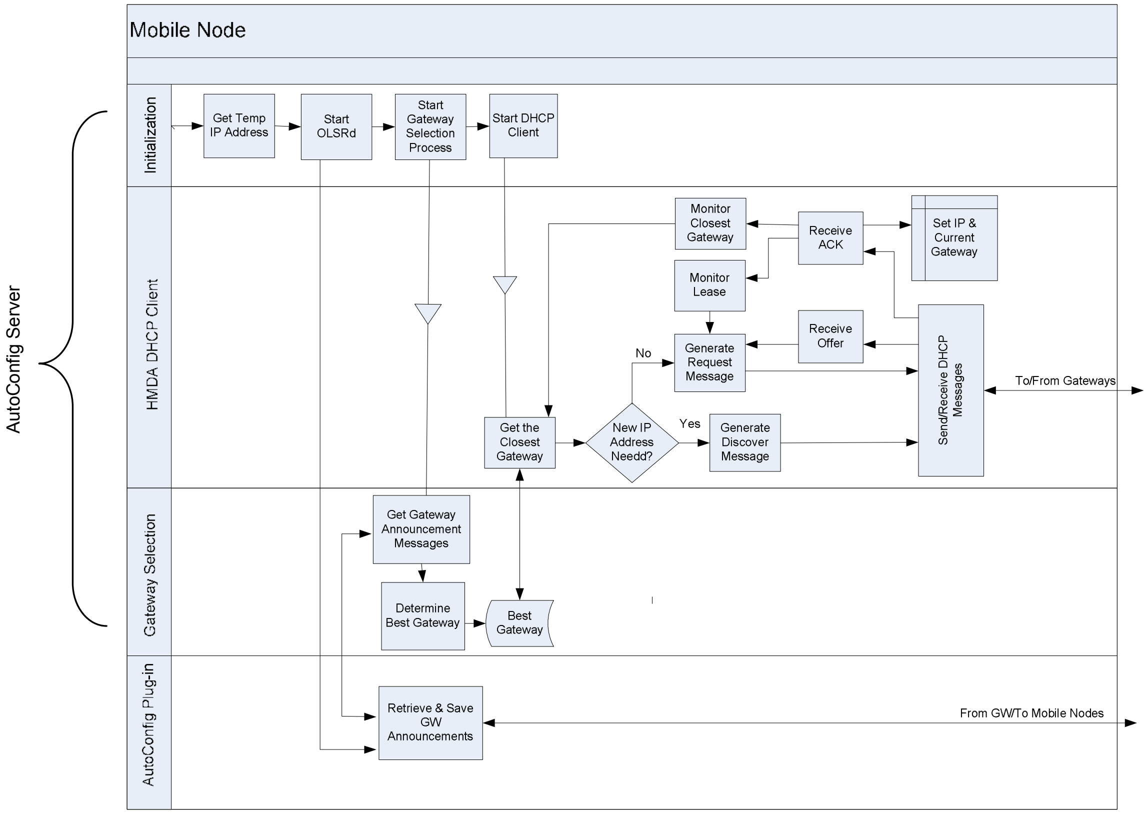

Figure 4.2.1-1 HMDA Mobile Node Components

The Initialization function performs the initial startup sequence of assigning the mobile node a temporary IP address from the Internet Assigned Number Authority (IANA), 169.254.0.0/16 subnet for host autoconfiguration. This is done to allow the mobile node to join the MANET and start receiving Gateway Announcement messages.

Once a temporary IP address has been assigned, OLSRd is started. OLSRd then initializes a process in the AutoConfigPlug-in software that periodically retrieves and stores Gateway Announcement message information. Gateway Announcement messages include the gateway IP address and its associated hop count.

The next step in the Initialization function is to start a Gateway Selection process where Gateway Announcement messages are retrieved from the AutoConfigPlug-in on periodic basis and the Best Gateway (GW) (closest as determined by the fewest hop counts) is stored. The Best GW information is updated every time the Get Gateway Announcement Messages process is run (currently configured to every 5 seconds).

The final Initialization function is to start the HMDA DHCP Client process. The HMDA DHCP Client process is responsible for monitoring the Best GW information stored in the Gateway Selection function and initializing the appropriate DHCP messages. The Get Closest Gateway process will determine what type of DHCP message should be sent to the gateway. The conditions which determine if a Discover or Request DHCP message is sent are as follows:

- Check to see if there is a previously assigned global IP address. If so, check to see if the associated gateway can be heard. If the associated gateway **can** be heard, generate and send a Request Message to that gateway.

- Check to see if there is a previously assigned global IP address. If so, check to see if the associated gateway can be heard. If the associated gateway **cannot** be heard, Get the Closest Gateway and generate and send a Discover message to that gateway.

- If only the temporary IP address exists, Get the Closest Gateway and generate and send a Discover message to that gateway.

The HMDA DHCP Client sends the DHPC Discover and Request messages to the appropriate gateway AutoConfigServer via OLSRd. When a DHCP Offer message is received in response to a DHCP Discover message, the HMDA DHCP Client generates a DHCP Request message in reply.

When a DHCP Ack is received, several events are triggered. The global IP address received in the DCHP Ack message and associated gateway is recorded in memory. A service is started to monitor the lease of the IP address. When the IP address lease time has expired, a DHCP Request message will be sent.

Once a DHCP Ack message is received, the HMDA DHCP Client function settles into a monitoring process in which the closest gateways will be monitored for Gateway Announcement messages. For the condition where the selected gateway can no longer be heard, the process starts again.

4.2.2 Gateway HMDA Functions

The AutoConfigServer and AutoConfigPlug-in software installed on the gateways are, like the mobile nodes, essentially a set of processes and services running in parallel. Initialization of the gateway HMDA functions begins by starting OLSRd. When OLSRd is started it initializes a process in the AutoConfigPlug-in software that periodically sends Gateway Announcement messages in accordance with the parameter, xinterval, that can be set in the *olsrd.conf* file. The OLSRd header of the Gateway Announcement message includes the following parameters; gateway IP address, Time to Live (TTL), and vtime, (time in seconds the message is valid within the MANET) which is also set in the *olsrd.conf* file.

The AutoConfServer processes are then started to control and manage DHCP messages. The HMDA AutoConfigServer consists of two functional components that are both processes managing DHCP messaging. The Manage Mobile Node DHCP Messages function listens for and receives DHCP Discover and Request messages from the mobile nodes and sends the DHCP Offer and Ack responses back to the requesting mobile node. The Manage DHCP Server Messages function is responsible for communications with the DHCP Server.

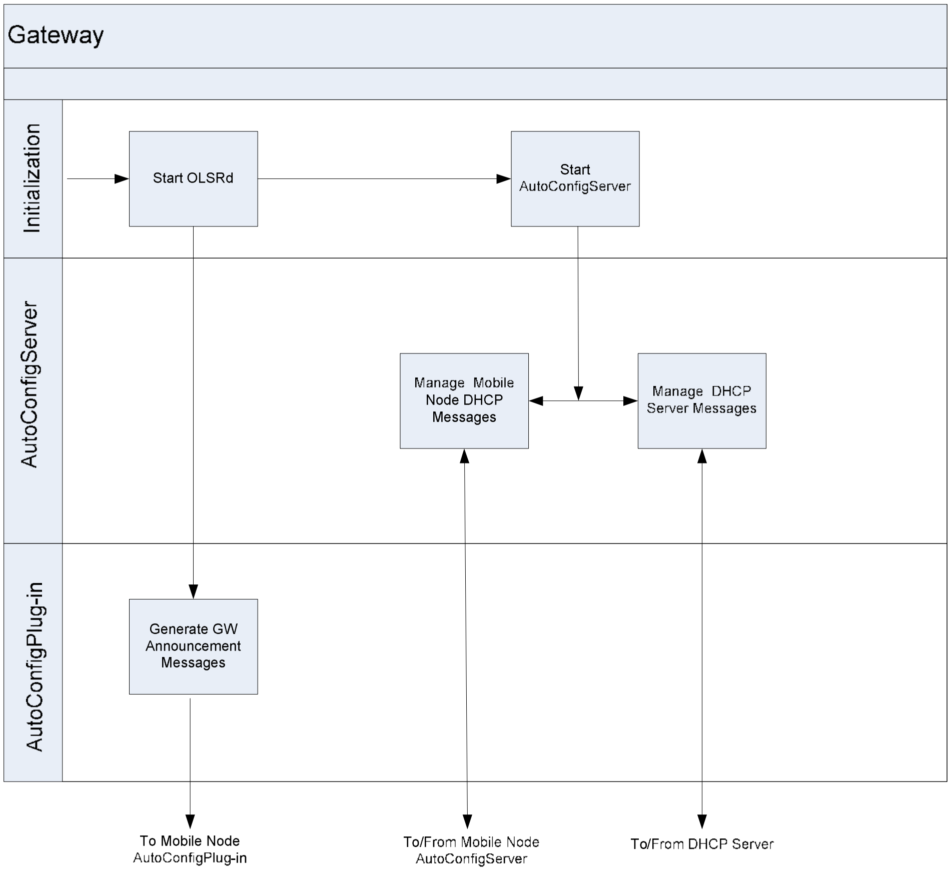
Gateway
Initialization
AutoConfigServer
AutoConfigPlug-in
Start OLSRd
Start AutoConfigServer
Manage Mobile Node DHCP Messages
Manage DHCP Server Messages
Generate GW Announcement Messages
To Mobile Node AutoConfigPlug-in
To/From Mobile Node AutoConfigServer
To/From DHCP Server

Figure 4.2.2-1 HMDA Gateway Components

5.0 Test Results

The HMDA Software Test Plans/Procedures (STPP) document was developed to verify HMDA Software Requirement Specification (SRS) requirements. These test procedures were run on version 0.01 of the HMDA AutoConfigServer and AutoConfigPlug-in SCIs. A discussion of the formal and ad-hoc test activities and results is provided in this section.

5.1 Formal Testing

The following paragraphs describe the tests performed and results obtained from formal testing. The following paragraphs reference the test steps and results identified in HMDA-STPP-01-U-ROC1.

Test 1 – Hardware/Software Configuration Test

Purpose: The purpose of this test was to verify correct installation and versioning of the application and test software on the mobile nodes, gateways, and DHCP servers. The SRS requirements that were verified in this test included:

- Requirement 12: The Hybrid MANET Dynamic Addressing Protocol shall include a Routing function that facilitates node to node communications via an Optimized Link State Routing (OLSR) protocol.

- Requirement 13: The Hybrid MANET Dynamic Addressing Protocol shall be demonstrated and tested using two gateways and four mobile nodes.

General Description: The HMDA User's Manual (UM) was used to completely re-build the mobile nodes, gateways and DHCP Servers. The test procedure was used to verify correct software and hardware installation and configuration. A specific network topology as shown in Figure 5.1-1 was configured using a script called *myiptables* which used a Linux command, "iptables" to define the routing topology for each mobile node and gateway. Once this was completed, the MANET and HMDA software was turned on and the routing table for each node was examined to verify correct network topology.

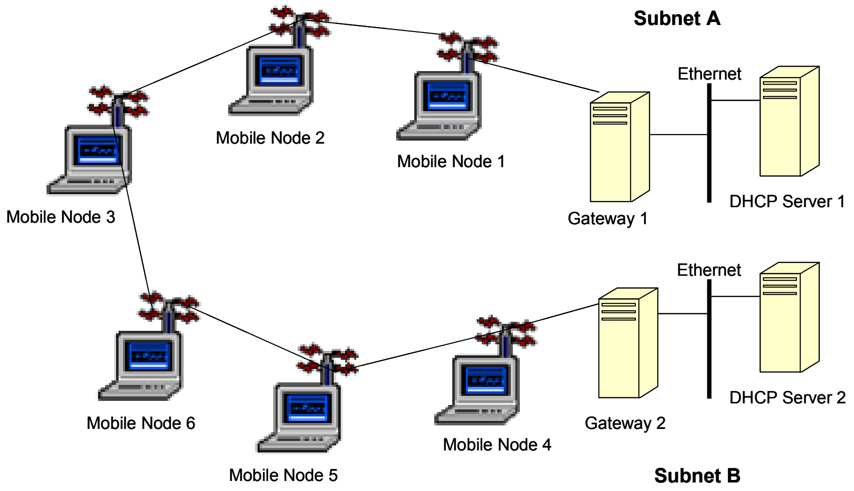

Figure 5.1-1 Hardware/Software Configuration Test Network Topology

Discussion of Results: The results of the Hardware/Software Configuration Test successfully verified both requirements. Although the first requirement was to verify HMDA using only four mobile nodes, an additional two mobile nodes were added in order to provide a more robust test and evaluation environment. As stated previously, the use of the "iptables" command was used to develop a script unique to the HMDA test environment called *myiptables* in order to emulate the wireless routing topology shown in Figure 5.1-1. This is required in the laboratory environment because of the close proximity of the mobile nodes and gateways. Without the *myiptables* file, all gateway and mobile nodes are one hop away from each other making it difficult to test many of the multi-hop related requirements associated with HMDA. The HMDA *myiptables* file shown in Figure 5.1-1a is for a network topology in which all nodes can "see" each other in the MANET. The fact that all "iptables" commands are commented out (i.e., # sign is inserted before the command) means that the node associated with a given Media Access Control (MAC) address will not be dropped from the network. The *myiptables* file is unique for each node in the network with respect to which nodes can be "heard". The MAC addresses represented in this figure reflect the MAC addresses of the mobile node and gateway wireless cards purchased under this contract. For example, gateway 1's *myiptables* file would only have the first line (gateway 1 "iptables" command) and line 3 (mobile node 1 "iptables" command) commented out indicating that gateway 1 can only hear itself and mobile node 1. Mobile node 1's *myiptables* file would have the "iptables" commands for gateway 1, mobile node 1, and mobile node 2 commented out, thus instantiated the connections for mobile node 1.

```
#! /bin/bash

#iptables -A INPUT -m mac --mac-source 00:14:6C:2F:12:24 -j  DROP# Gateway 1
#iptables -A INPUT -m mac --mac-source 00:14:6C:72:6A:FA -j DROP# Gateway 2
#iptables -A INPUT -m mac --mac-source 00:14:6C:06:85:21 -j  DROP# Mobile Node 1
#iptables -A INPUT -m mac --mac-source 00:18:4D:8E:C4:98 -j DROP# Mobile Node 2
#iptables -A INPUT -m mac --mac-source 00:18:4D:9E:A9:39 -j DROP# Mobile Node 3
#iptables -A INPUT -m mac --mac-source 00:14:6C:1F:03:6A -j DROP# Mobile Node 4
#iptables -A INPUT -m mac --mac-source 00:14:6C:1F:07:76 -j DROP# Mobile Node 5
#iptables -A INPUT -m mac --mac-source 00:14:6C:F8:88:28 -j DROP# Mobile Node 6
```

Figure 5.1-1a HMDA *myiptables* File

Once the simulated network topology was established on all of the network node elements, the HMDA (and OLSRd) software was started. Test Steps 30 – 45 verify that the network topology is recognized and implemented by the OLSRd routing function. In addition, Test Step 1 verified that OLSRd was installed on the nodes. It is important to recognize that the startup sequence for the gateways and mobile nodes must be followed for correct test operation and results.

Test 2- Gateway Management and Mobile Node Initialization Test

Purpose: The purpose of this test is to demonstrate the capability for an administrator to create a unique address block and lease assignments for each gateway. This test also demonstrates the capability of each mobile node to obtain a valid IP address soon after power-up. The SRS requirements that were verified in this test included:

- Requirement 4: The Hybrid MANET Dynamic Addressing Protocol shall include a Gateway Manager function that allows each gateway to maintain and distribute IP addresses to mobile nodes.

- Requirement 5: The Gateway Manager function shall provide configuration control of the IP address block by providing for the reclamation of IP addresses that are no longer in use.

- Requirement 6: This function shall also provide a configurable leasing function that allows a mobile node to retain an IP address for a given period of time.

- Requirement 7: The Gateway Manager function shall provide the capability for an administrator to create a unique address block for each gateway.

- Requirement 10: The Hybrid MANET Dynamic Addressing Protocol shall include an Address AutoConfig function that enables a mobile node to obtain a valid global IP address associated with the chosen gateway soon after power-up.

General Description: This test was conducted by modifying the IP address block and lease assignments in the *dhcpd.conf* file (generated by the ISC DHCP software) and verifying that the mobile node HMDA DHCP clients correctly enter the binding states and complete the DHCP "Discover/Offer/Request/Ack" handshake that is required by Request For Comment (RFC) 2131. Figure 5.1-2 identifies the network topology used for this test.

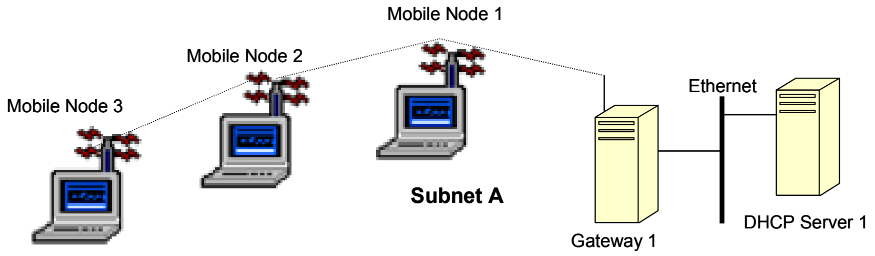

Figure 5.1-2 Gateway Mobile Node Initialization Test Network Topology

Based on the fact that the requirements for this test are placed primarily on the DHCP Server selected for the HMDA configuration, only three mobile nodes were used to verify these requirements in what should be described as more of a demonstration that the HMDA software interacts smoothly with the DHCP server rather than HMDA functional verification. Focus was placed on how the user interacts with the DHCP sever to provide proper IP address blocks and lease times for mobile nodes in the MANET.

Upon opening the *dhcpd.conf* file, it should be noted that the shared-network MANET block has been modified from the norm in order to accommodate the DHCP server being on a neighboring subnet (via Ethernet connection). The subnet was expanded to include any address in the last two octets thereby joining the MANET subnet (192.168.2.any number from 0 to 255) with the DHCP server on the Ethernet subnet (192.168.1.x for gateway1 or 192.168.3.x for gateway 2). This expansion shows up in the *dhcpd.conf* file as 192.168.0.0 for the subnet and similarly 255.255.0.0 for the netmask. This now allows the DHCP server to provide addresses for the MANET in whatever ranges the user desires (e.g. 192.168.2.4 -192.168.2.30).

It should also be noted that our HMDA DHCP Client does not currently request a specific IP address lease time and therefore will obtain the default-lease-time. This is in contrast to the ISC DHCP client that comes bundled with openSUSE10.1 which always requests an infinite lease time and will therefore obtain the max-lease-time.

Discussion of Results: The results of the Gateway Management and Mobile Node Initialization Test successfully verified all of its requirements. The mobile nodes upon power-up and start-up of the HMDA software obtained a proper global IP address within the address block of the DHCP server thereby verifying requirement 10. Then the tester edited the *dhcpd.conf* file to create a unique address block and to set the new lease times.

When the mobile nodes were restarted, they received IP addresses within the new address block of the DHCP server thereby verifying requirements 4 & 7.

Mobile node 1 renewed its lease properly thereby verifying requirement 6.

Requirement 5 is the responsibility of the DHCP server because once a lease is up for a mobile node and the mobile node does not renew that lease, the DHCP server reclaims the lease as required by RFC 2131.

Test 3 – Gateway Announcement and Discovery Test

Purpose: The purpose of this test is to demonstrate the capability of each gateway to make periodic Gateway Announcement messages via the routing function providing gateway identity and selection parameters to mobile nodes. This test also verifies that the Gateway Announcement message includes a configurable TTL Parameter. The SRS requirements that were verified in this test included:

- Requirement 2: The Hybrid MANET Dynamic Addressing Protocol shall include a Gateway Discovery function that enables mobile nodes to receive gateway announcements over the hybrid MANET

- Requirement 8: The Gateway Manager function shall make periodic gateway announcements via the Routing Function providing gateway identity and selection parameters.

- Requirement 9: The Gateway Manager function shall provide the capability to configure the time to live for gateway announcements.

General Description: This test was conducted by modifying gateway 1's TTL and xinterval parameters in the *olsrd.conf* file. The TTL parameter contains the maximum number of hops a Gateway Announcement message will be transmitted. The default value for TTL is eight hops. The xinterval parameter defines how often the Gateway Announcement message will be broadcast over the MANET. The default value for xinterval is ten seconds. The network topology used for this test is identified in Figure 5.1-3. The value for TTL was changed to two hops and the xinterval value was changed to 5 seconds during conduct of this test. Ethereal was used to verify the frequency of the Gateway Announcement messages. A test script *dhcpprcclient.py* was run on the mobile nodes to record hop count.

A note here on the difference between the way hops are counted for the TTL parameter and the way the *dhcpprcclient.py* test script displays hops. Both are generated and used by the OLSRd software. The *dhcpprcclient.py* obtains the value for hop counts and TTL from the OLSRd header before those values are modified (i.e., the hop count is incremented and TTL is decremented) and broadcast to other mobile nodes. When an OLSRd packet is received by a mobile node with a TTL value of 0, the packet is dropped. Referring to the test setup, Gateway Announcement messages from gateway 1 will reach mobile node 1 when the TTL is set to 1. When the *dhcpprcclient.py* test script on mobile node 1 is run, it will show the hop count to be 0. This relationship will remain the same for mobile nodes further away from the gateway, e.g. a TTL of 3 will reach mobile node 3 but not mobile node 4 and if the *dhcpprcclient.py* test script is run on mobile node 3, it will show a hop count of 2. There is a hop count variable used within the AutoConfigServer to calculate the closest gateway. This variable was not created to measure hop counts. The *dhcpprcclient.py* is capturing the hop count value generated by OLSRd software before the hop count value is incremented by OLSRd.

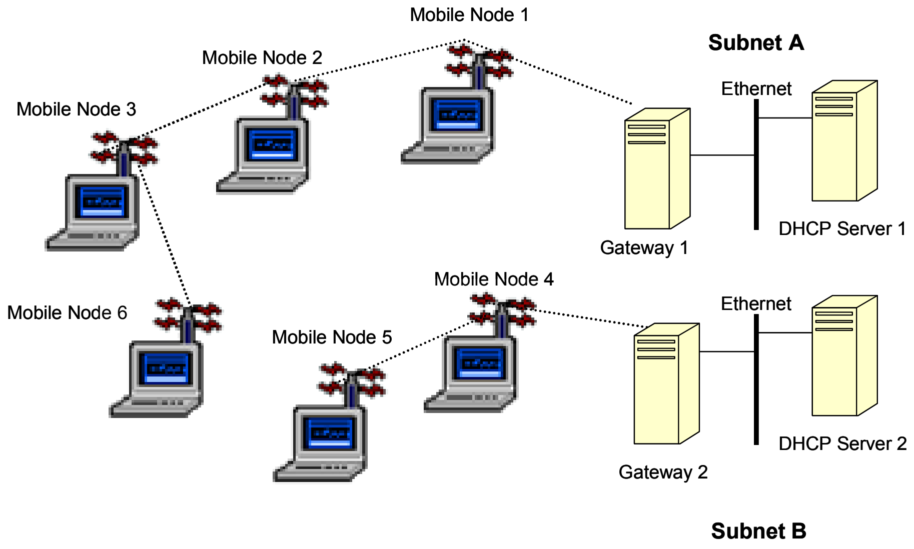

Figure 5.1-3 Gateway Announcement and Discovery Test Network Topology

Discussion of Results: The results of the Gateway Announcement and Discovery Test verified all of its requirements. Running the *dhcpprcclient* script indicated that the mobile nodes were receiving Gateway Announcement messages implying that the gateways were sending Gateway Announcement messages thus verifying requirement 2. The *dhcpprcclient* script also displayed the gateway identity information that the Gateway Announcement message provided verifying part of requirement 8. The information obtained from Ethereal confirmed that the Gateway Announcement messages were sent periodically in accordance with the time that was set in the *olsrd.conf* file verifying another portion of requirement 8.

By setting the TTL parameter in the *olsrd.conf* file to two, one can see its effect on path length. The first two mobile nodes received Gateway Announcement messages and the last two mobile nodes (mobile node 3 and mobile node 6) did not receive the messages. This procedure verifies requirement 9 and completes the verification of requirement 8.

Test 4 – Mobile Node Reconfiguration and Gateway Selection Test

Purpose: The purpose of this test was to demonstrate the capability of a mobile node to evaluate and select an appropriate gateway based on hop counts and the capability of a mobile node to obtain a valid IP address when the existing IP address becomes invalid and through gateway reselection. The SRS requirements that were verified in this test included:

- Requirement 3: The Hybrid MANET Dynamic Addressing Protocol shall include a Gateway Selection function that allows mobile nodes to evaluate and select an appropriate gateway based on quality of service metrics to include at a minimum, hop counts.

- Requirement 11: This function shall also provide the capability for a mobile node to obtain a new IP address if the existing IP address becomes invalid or through gateway reselection.

General Description: This test was conducted by using a test script, "dhcpprcclient" to identify the closest gateway to each mobile node and then turning each mobile node off and then back on to verify that the mobile node correctly selected the gateway with the fewest hops. The network topology used for this test is shown in Figure 5.1-4. A second test is performed by turning off gateway 1 and verifying that mobile nodes 1, 2, and 3 acknowledge that gateway 1 Gateway Announcement messages are no longer being heard and request new IP addresses from gateway 2. Gateway 1 is then restarted and a check is performed to verify that mobile nodes 1, 2, and 3 do not request new IP Address from gateway 1. A final check is conducted by changing the TTL parameter in the olsrd.conf file in gateway 2 to three hops and verifying that mobile nodes 1, 2, and 3 recognize that gateway 2 Gateway Announcement messages are no longer being received and request new IP addresses from gateway 1.

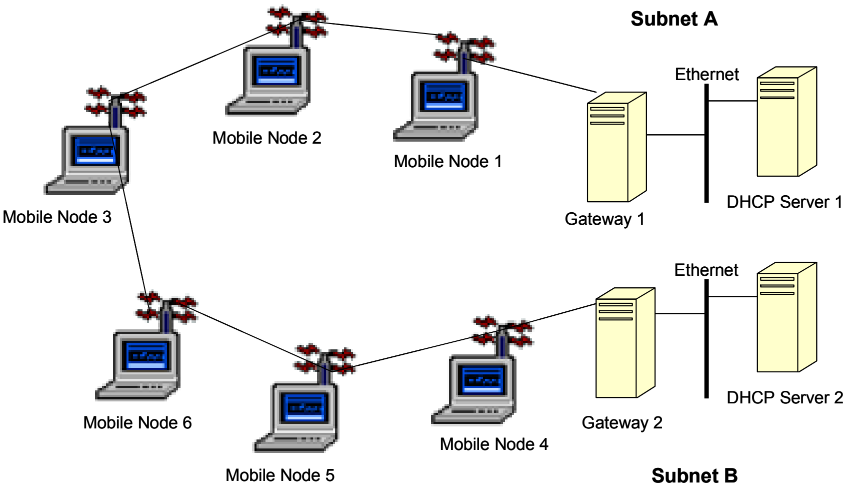

Figure 5.1-4 Mobile Node Reconfiguration and Gateway Selection Test Network Topology

Discussion of Results: The results of the Mobile Node Reconfiguration and Gateway Selection Test verified both of its requirements. The IP address assignments received by the mobile nodes in the initial power-up may reflect more the order that the mobile nodes are started than which gateway is closer. The next test steps provide a definitive method to confirm that each mobile node chooses the gateway that is the fewest hops away. When each mobile node is shut down, reset, and then restarted, the examination of the IP address allowed the determination of which DHCP server provided the IP address and its associated gateway. Then by examination of the information provided by the *dhcpprcclient.py* script, it could be confirmed that the mobile node chose the closest gateway. This process verifies requirement 3.

When gateway 1 was shut down, mobile nodes 1, 2, and 3 could no longer hear from this gateway and correctly switched to gateway 2. This verifies requirement 11 (and thereby satisfying all the requirements).

Gateway 1 was then re-started to test whether the mobile nodes closer to gateway 1 exhibited a tenacious hold on their IP addresses i.e., whether they keep their IP address even if they hear from a gateway that is closer. Mobile nodes 1, 2 & 3 correctly retained their IP addresses associated with gateway 2, thereby confirming tenacity. By changing the TTL on gateway 2 to 3, we provided another scenario in which mobile nodes 1, 2 and 3 would not hear from a gateway, i.e. a mobile node may move too many hops from its current gateway and need to switch to another gateway that it hears. Mobile nodes 1, 2 and 3 no longer could hear from gateway 2 and successfully switched to gateway 1.

5.2 Expanded Testing

In addition to the functional testing performed to verify HMDA SRS requirements, expanded testing was required to verify design goals and expected performance aspects of HMDA.
These tests included:

- Communications between mobile nodes without gateways

  The network configuration identified in Figure 5.1-4 was used for this test. All six mobile nodes were turned on and were receiving Gateway Announcement messages from both gateways. Then, both gateways were turned off. Running "dhcpprclient" verified that none of the mobile nodes were receiving Gateway Announcement messages. It was also verified that the mobile nodes maintained their current IP Addresses even when they couldn't hear any gateways. They were capable of routing packets to each other thereby satisfying the rest of design goal 9.

- HMDA DHCP Client Testing

  Additional testing was required to verify that the HMDA DHCP Client met RFC 2131 client requirements. We are confident that our HMDA DHCP Client will interface correctly with other commercial versions of a DHCP server. However, there were some mandatory DHCP client requirements that were intentionally excluded in the HMDA DHCP Client implementation.

- The HMDA DHCP Client does not include the functionality to produce DHCPDECLINE messages. Incorporation of this message type may not be applicable to a Hybrid MANET over a low bandwidth network. The DHCPDECLINE message defines a requirement for the DHCP Client to first send out an Address Resolution Protocol (ARP) message over the MANET to determine if the IP Address offered by the DHCP Sever is already in use. If a response back over the MANET confirms that the IP Address offered by the DHCP Server is in use by another node or device, the DHCP Client is required to send a DHCPDECLINE message to the DHCP Server refusing the offered IP Address. Although this functionality can be added to the HMDA DHCP Client, more research should be conducted to determine if the added traffic for the ARP messages can be accommodated or even desirable for the operation scenario.

- The HMDA DHCP Client does not include the functionality to produce DHCPINFORM messages. This message type is generated when a mobile node wants parameters that are appropriate for the network segment that the mobile node claims to be connected. Although this functionality can be added to the HMDA DHCP Client, further discussions with potential users is advised to determine if this function is desirable for a HMDA operational scenario.

- The HMDA DHCP Client does not include the functionality to produce a DHCPRELEASE message. Again, the concern here is that a DHCPRELEASE message may not be applicable within the operational scenario defined for HMDA. Specialized use cases defining when a mobile node should release its IP address should be developed prior to implementation.

- The HMDA DHCP Client does not follow RFC 2131 requirement to stop processing if an IP address lease expires before an ACK is received by the DHCP server. This requirement conflicts with the requirements and design goals for the mobile nodes to maintain communications within the MANET if no gateways are heard.

6.0 Conclusion

The HMDA system is a proof–of-concept solution that meets the contractual requirements and satisfies section 3 design goals. The solution has been developed and tested in a laboratory environment. As such there are still areas in both software development and testing that can be improved when the HMDA system is transitioned to an operational phase.

HMDA provides the capability for a mobile node to get a global IP address from the closest gateway/DHCP server upon power-up. HMDA then monitors that gateway and its IP address lease time. When the mobile node no longer hears from its gateway for a specified length of time, the mobile node will then obtain a new IP address from the closest gateway it hears. When the mobile node nears its IP address lease expiration time, it will then renew its lease.

A current feature of HMDA is to ensure that the mobile node retains its IP address even if a closer gateway is heard (a property call tenacity). The mobile node will also keep its IP address even when no gateways are heard. This allows the mobile nodes to communicate with each other when in range.

HMDA provides the capability for a system administrator to configure the parameters of the Gateway Announcement messages to support any operational scenario. These parameters define the gateway IP address, the transmission frequency, the time to live in hop counts, and the length of time in which the message is valid (validity time). The transmission frequency provides for control of the overhead traffic associated with the generation of Gateway Announcement messages. Tradeoffs between overhead and timeliness of receipt must be considered when increasing or decreasing the frequency in which Gateway Announcement messages are generated. The TTL parameter provides for control of the range the Gateway Announcement message can travel through the MANET. Again trade-offs must be made as to how large to make the range (TTL) within the MANET. A large TTL may result in poor communication links due to degradation over many hops. A TTL that is too small may result in nodes not being able to obtain a global IP address. The validity time provides for control of the length of time the Gateway Announcement messages stays in the MANET.

Certain algorithms cannot be adequately tested in a laboratory environment and need to be exercised in an operational-like environment. This would involve using a greater number of mobile nodes and gateways in a more complex network, as well as injecting electromagnetic interference. A harsher environment can be simulated by manipulation of the transmit power.

The gateway selection methodology should be expanded beyond just selecting the gateway that is the fewest hops away and holding onto that gateway until it is no longer “heard”. An improved method may be obtained by viewing gateway selection as analogous to a radio receiver selecting the strongest signal. As the radio keeps a history of signals received, the mobile node could keep a history of gateways received along with relevant information with regards to network performance. The receiver has electronics to analyze the received signal history and predict the strongest/best signal. Likewise, the mobile node could incorporate software that analyzes the received gateway history and network performance parameters in order to predict the best gateway.

This gateway selection methodology is dependent on the operational scenario. A major timing consideration is how long it takes to propagate (defined as x) the new global IP address to the world. For example, the limiting time for a mobile node to obtain a better gateway is a multiple of x. After that limiting time, the mobile node can switch gateways. Factors that can increase or decrease the propagation time, thus affecting network performance, are dependent on system network components outside of the MANET. Protocols such as the Host Identify Protocol (HIP) could theoretically improve network performance by decreasing the propagation time.

Security issues involving confidentiality, integrity and availability were not addressed and considered beyond the scope of this effort. For example, the HMDA User's Manual requires that all firewalls be disabled. This is not acceptable in an operational environment where firewall rules must exist to ensure availability of the network. Also, a method for message and data encryption must be considered in order to provide for confidentiality and integrity of the network.

SAIC has successfully implemented and demonstrated the Network Monitoring and Management Hybrid MANET Dynamic Addressing concept that meets or exceeds the requirements and objectives set forth by ONR. Since positive test results were obtained, it is recommended to transition this methodology from the lab environment to an operational scenario.

7.0 Acronyms, Abbreviations, and Definitions

API	Application Programming Interface
ARP	Address Resolution Protocol
BOOTP	Bootstrap Protocol
DHCP	Dynamic Host Configuration Protocol
GW	Gateway
HIP	Host Identity Protocol
HMDA	Hybrid MANET Dynamic Addressing
IANA	Internet Assigned Numbers Authority
IP	Internet Protocol
IPC	Inter-Process Communication
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISC	Internet Software Consortium
LAN	Local Area Network
MAC	Media Access Control
MANET	Mobile Ad-Hoc Network
OLSR	Optimized Link State Routing
ONR	Office of Naval Research
RFC	Request for Comment
SAIC	Science Applications International Corporation
SCI	Software Configuration Item
SMF	Simplified Multicast Forwarding
SRS	Software Requirements Specification
STPP	Software Test Plans/Procedures
STR	Software Test Report
TCP	Transmission Control Protocol
TTL	Time to Live
UDP	User Datagram Protocol
UM	User’s Manual